IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MINTEL INTERNATIONAL GROUP, LTD, a United Kingdom corporation,	)	
Plaintiff,	)	Case No.: 08 CV 3939
v.	)	Judge Robert M. Dow
	)	Magistrate Judge Maria Valdez
MEESHAM NEERGHEEN, an individual,	)	
Defendant.	)	

MOTION TO COMPEL DATAMONITOR'S COMPLIANCE WITH SUBPOENA

Plaintiff MINTEL INTERNATIONAL GROUP, LTD. ("Mintel") hereby moves this Court to compel Datamonitor to provide all documents and things responsive to the July 21, 2008 Subpoena for Documents to Datamonitor ("Datamonitor Subpoena"). In support of its motion, Mintel states as follows:

1. On or about July 11, 2008, Mintel filed a Complaint for Injunctive and Other Relief against Defendant Meesham Neergheen ("Defendant"), alleging violation of the Illinois Trade Secret Act, Computer Fraud and Abuse Act, and violation of various terms of Defendant's employment contract and non-compete agreement. It is Mintel's contention that Defendant is in violation of his non-compete agreement because Defendant is currently working for Datamonitor, a direct competitor of Mintel.

2. On July 15, 2008, opposing counsel filed an appearance on behalf of Defendant.[1] In addition, on that date, the Court conducted an emergency hearing on Mintel's request for a temporary restraining order.

3. On July 16, 2008, the Court granted in part and denied in part Mintel's motion for a temporary restraining order. More specifically, the Court order stated as follows:

> C. Defendant is required to return to Mintel all copied, printed, and/or downloaded files, materials, and information taken from Mintel;
> D. Defendant is required to produce forensic copies of all personal desktop and/or laptop computers;
> E. Defendant, his agents, servants, employees, officers, attorneys, successors and assigns, and all persons, firms, and corporations acting in connection or participation with him or on his behalf, are prohibited from deleting any files from Defendant's personal desktop and/or laptop computer related to or taken from Mintel.

See July 16, 2008 Order.

4. Although the Temporary Restraining Order was entered by the Court on July 16, 2008, Defendant did not turn over his computer to his counsel and/or forensic expert until July 18, 2008. In fact, Defendant continued using his computer through the morning of July 18, 2008. Defendant continued to use his computer despite having knowledge on July 11, 2008 of the pending litigation when Defendant received notice of the emergency hearing and received a copy of the Complaint for Injunctive and Other Relief. Furthermore, Defendant continued to use his computer despite the Court entering the Temporary Restraining Order on July 16, 2008, which required Defendant to turn over all personal computers for forensic imaging.

---

[1] However, it is important to note that opposing counsel also represents Datamonitor. In fact, Defendant conceded during his deposition that Datamonitor hired opposing counsel for him and that Datamonitor is paying all fees, including attorney fees, associated with this lawsuit. *See* Exhibit 2, 49:3-24.

5. Defendant's use of his computer on and after July 11, 2008 is clearly inconsistent with Defendant's duty to preserve evidence – such duty arising upon Defendant's notification of the litigation in question. This Court has made clear that a formal discovery request is not necessary to trigger the duty to preserve evidence. *Danis v. USN Communs., Inc.*, 2000 U.S. Dist. LEXIS 16900, at * 33 (N.D. Ill. Oct. 23, 2000). Instead, the filing of a complaint alerts a party that certain information is relevant and likely to be sought in discovery. *Cohn v. Taco Bell Corp.*, 1995 U.S. Dist. LEXIS 12645, at * 5 (N.D. Ill. Aug. 30, 1995).

6. Therefore, after receiving a copy of the Complaint, Defendant was alerted to the fact that the contents of his personal computer would likely be relevant evidence in the legal action against him. Furthermore, after receiving a copy of the Complaint on July 11, 2008, Defendant had a duty not to alter, destroy or modify the contents of his personal computer. Even if Defendant pleads ignorance and claims Defendant was not aware of his duty to preserve all relevant evidence, opposing counsel filed an appearance on behalf of Defendant on July 15, 2008. Furthermore, the Temporary Restraining Order was entered on July 16, 2008, which made clear that Defendant was to provide forensic images of all personal computers and refrain from deleting any files related to or taken from Mintel. Therefore, any argument by Defendant that he was unaware of his duty to preserve evidence on or after July 15, 2008 is completely without merit and should be disregarded by the Court.

7. Not only did Defendant improperly continue to use his personal computer after July 11, 2008, but as the attached affidavit of Scott Jones of Forensicon makes clear, Defendant has taken deliberate action to destroy evidence within the pending case. A party

has a duty to preserve evidence, including any relevant evidence over which the party has control and reasonably knew or could reasonably foresee is material to a potential legal action. *China Ocean Shipping Co. v. Simone Metals*, 1999 U.S. Dist. LEXIS 16229, at * 2 (N.D. Ill. Oct. 1, 1999); *see also Boyd v. Travelers Ins. Co.*, 166 Ill. 2d 188 (Ill. 1995). Spoliation of evidence occurs when one party destroys evidence relevant to an issue in the case. *Smith v. United States*, 293 F.3d 984, 988 (7th Cir. 2002) (citing *Crabtree v. Natl. Steel Corp.*, 261 F.3d 715, 721 (7th Cir. 2001)). Fault may be evidenced by negligent actions or a flagrant disregard of the duty to preserve potentially relevant evidence. *Diersen v. Walker*, 2003 U.S. Dist. LEXIS 9538, at * 5 (N.D. Ill. June 6, 2003).

8. As is evident by the Jones Affidavit, the core evidence of destruction by Defendant include:

- The continued usage of the computer even after Defendant was notified on July 11, 2008 of the present litigation;
- The creation and deletion of files and folders, including Windows registry data, after notice of active litigation;
- The deletion of Internet history data for much of the time period prior to July 14, 2008;
- The usage of utilities to further obscure dates and times related to files such as antivirus software; and
- The usage of the Windows defragmentation utlity on July 14, 2008 to make deleted file data evidence unrecoverable.

See Jones Affidavit, ¶ 4, attached hereto as "Exhibit 1."

9. More specifically, Defendant deleted approximately 98 file entries following his receipt of the Complaint until as recently as July 18, 2008. *See* Exhibit 1, ¶ 11. Defendant also created 3,900 new file entries on or after July 13, 2008. *See* Exhibit 1, ¶ 11. Until such a time that deleted file data is overwritten by new file data, it is generally recoverable and available for review. *See* Exhibit 1, ¶ 11. Therefore, creating new file entries after deleting files is commonly done by users to destroy evidence of past activities, including the existence or usage of files. *See* Exhibit 1, ¶ 11. Although Defendant testified during his deposition that he did not delete any documents, it is clear that Defendant deleted file data from his computer after receiving notification of active litigation. *See* Exhibit 1, ¶ 11; *see* Neergheen Deposition, p. 48:17-21, attached hereto as "Exhibit 2."

10. Furthermore, Defendant's McAfee antivirus program continued to run on Defendant's computer through July 18, 2008. *See* Exhibit 1, ¶ 13. Defendant's continued usage of antivirus software up until the date of forensic imaging obscured the dates and times when file entries were accessed and further destroyed evidence related to dates and times which would exist if not for the usage of the antivirus software. *See* Exhibit 1, ¶ 13. If Defendant would have left his computer alone starting on July 11, 2008, the antivirus software would not have been able to alter time and date metadata for any of the file entries. *See* Exhibit 1, ¶ 13. "Once a party is on notice that files or documents in their possession are relevant to pending litigation, the failure to prevent the destruction of relevant documents crosses the line between negligence and bad faith, even where the documents are destroyed according to a routine document retention policy. *Siginton v. CB Richard Ellis*, 2003 U.S. Dist. LEXIS 19128, at *7 (N.D. Ill. Oct. 23, 2003). "Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy." *Krumwiede v.*

Brighton Associates, LLC, 2006 U.S. Dist. LEXIS 31669, at * 23 (N.D. Ill. May 8, 2006) (citing *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003)). Therefore, even giving Defendant the benefit of the doubt and assuming the antivirus software ran automatically and was not initiated by Defendant, Defendant was nonetheless under an affirmative obligation to ensure the preservation of relevant documents. Therefore, Defendant should not have even turned on his computer after receiving notice of the litigation on July 11, 2008. Or, at a very minimum, Defendant should have suspended the running of the antivirus software.

11. However, Defendant's spoliation of evidence does not end there. On July 17, 2008 Defendant searched Microsoft's support website for information related to deleting file data. *See* Exhibit 1, ¶ 18. Defendant admitted to visiting this website during his deposition. *See* Exhibit 2, p. 145:12-16. A simplified version of the query text entered by Defendant while at Microsoft's support website is included within Table Three in the Jones Affidavit. *See* Exhibit 1, p. 9. Furthermore, "Exhibit B" to the Jones Affidavit shows all the various topics Defendant could choose from when visiting Microsoft's support website, including the deletion of registry keys, the deletion of files and folders, and the deletion of internet files. *See* Exhibit 1, ¶ 22; *see also* Exhibit B to Exhibit 1. Not surprisingly, the information Defendant actively sought on July 17, 2008 regarding the destruction of evidence closely aligns to the evidence destruction found by Jones. *See* Exhibit 1, ¶ 22. Therefore, not only was Defendant's computer still being used on July 17, 2008, but Defendant was using the computer to search for information about how to delete data. And, Defendant was both searching for information on how to delete data and deleting data on July 17, 2008 in direct violation of the temporary restraining order entered on July 16, 2008.

12. As the Jones Affidavit makes clear, Defendant also purposefully deleted his Internet history. Defendant's computer is missing Internet history data that would report activity from the time period prior to Defendant's resignation from Mintel until after active litigation was filed. *See* Exhibit 1, ¶ 24. Not only are there gaps in Defendant's daily Internet history, but there is no weekly Internet history data for Defendant from January 23, 2008 through the date the computer was forensically imaged. *See* Exhibit 1, ¶ 24. Not surprisingly, it is common in misappropriation cases for a user to delete Internet history data, which would reflect notable actions such as the continued access and usage of emailed file data following one's departure from a company and after beginning employment with a competitor. *See* Exhibit 1, ¶ 27.

13. The Jones Affidavit also contains Windows Registry information related to storage devices that have been connected to Defendant's computer via the Universal Serial Bus ("USB"). *See* Exhibit 1, ¶ 28. On July 17, 2008, Defendant connected two separate devices to his computer. *See* Exhibit 1, ¶ 28. These devices can typically be used to both transfer and/or store file data. *See* Exhibit 1, ¶ 28. Not only did Defendant attach these two separate devices to his computer, but Defendant then deleted the information that is stored on the devices from Defendant's hard drive. *See* Exhibit 1, ¶ 34. Given the fact that Defendant deleted the USBSTOR registry report, it is impossible to determine from the forensic computer image the information stored on these devices. *See* Exhibit 1, ¶ 37. However, this leads to the inescapable conclusion that Defendant attempted to destroy evidence regarding storage locations to which Defendant likely copied and/or stored Mintel file data. *See* Exhibit 1, ¶ 32. The fact that the USBSTOR file entries report as being updated on the same day that Defendant searched for technical documentation on how to

access registry settings and delete data further supports Mintel's contention that the deletion was deliberate. *See* Exhibit 1, ¶ 32.

14. It is also important to note that Mintel has requested within its written discovery that Defendant produce all devices that Defendant connected to his personal computer, for these devices may also contain Mintel's confidential information as well. Although Defendant responded by stating he would produce all responsive items, Mintel has received no such devices to date. Based upon the Jones Affidavit, it is clear that Defendant has connected numerous devices to his computer, which not surprisingly contradicts Defendant's testimony that he has only used two such devices. *See* Exhibit 1, ¶ 37; *see also* Exhibit 2, pp. 96:3-97:9. Given the fact that Defendant deleted the USBSTOR registry report, it is impossible to determine from the forensic image the information stored on these devices. *See* Exhibit 1, ¶ 32. If Defendant has nothing to hide, then there is no reason for the delay Mintel has encountered in obtaining these devices.

15. On July 14, 2008, the Windows defragmentation utility was run on Defendant's computer. *See* Exhibit 1, ¶ 45. Again, this utility was used well after Defendant was served notice of the present litigation. "Defragmentation is a method to cover up deletions of data by eliminating all traces of deleted data." *RKI, Inc. v. Grimes*, 177 F. Sup. 2d 859, 875 (N.D. Ill. 2001). The use of the defrag utility after deleting file data is a commonly-employed means of rendering deleted file data forever unrecoverable in the file data's original native format. *See* Exhibit 1, ¶ 45. Once a deleted file is overwritten with new data, it is generally no longer recoverable or available for review in its original native format. *See* Exhibit 1, ¶ 46. Besides the usage of defrag to destroy evidence, other prefetch file entries report creation and/or being last written on July 17, 2008. *See* Exhibit 1,

¶ 48. This further file entry creation necessarily overwrites previously unallocated space which contained evidence. *See* Exhibit 1, ¶ 48. If not for the file creation activities which destroyed evidence, this previously-deleted file data would have been available for review. *See* Exhibit 1, ¶ 48. Therefore, Defendant destroyed additional evidence by using the defrag utility and creating prefetch file entries.

16. Based upon the evidence found by Jones, it is clear that Defendant acted willfully and in bad faith when he continued to alter, modify and destroy evidence after July 11, 2008. Beginning on July 11, 2008, Defendant had a duty not to alter, destroy or modify the contents of his computer. Despite this duty to preserve evidence, Defendant's computer experienced a spike in activity between July 11, 2008 and July 18, 2008, which resulted in the alteration, modification and/or destruction of thousands of potentially relevant files and their metadata. Particularly troubling is Defendant's continued use of the computer after Defendant's counsel filed an appearance on July 15, 2008. Furthermore, Defendant violated the express terms of the temporary restraining order by deleting and defragmenting his computer after the entry of the order on July 16, 2008. In fact, it appears that Defendant worked late on July 17, 2008 in order to complete as many file transfers, alterations and deletions as possible before relinquishing control of the computer. More specifically, Defendant worked until approximately 10:40 p.m. on July 17, 2008. Defendant conceded during his deposition that no other individuals, excluding his attorneys, had access to his computer on or after July 11, 2008. *See* Exhibit 2, pp. 93:22-94:4. Therefore, all activity that occurred on Defendant's computer was initiated and completed by Defendant himself

17. Despite Defendant's testimony during his deposition that he has not used any of Mintel's confidential information that he misappropriated, it is clear that based upon the

behavior of Defendant between July 11, 2008 until July 18, 2008, Defendant is not a credible individual. Defendant has clearly demonstrated a lack of candor and, therefore, Mintel should not be forced to rely upon Defendant's mere assertion that he has not used Mintel's confidential information to date. In other words, Defendant cannot "be trusted to act with the necessary sensitivity and good faith under the circumstances in which the only practical verification that he was not using plaintiff's secrets would be [defendant's] word to that effect." *Pepsico, Inc. v. Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995). Clearly, Defendant is not a trustworthy individual. Therefore, in order for Mintel to know whether Defendant has passed along Mintel's confidential information to Datamonitor or is using the information to the detriment of Mintel, Mintel should be permitted to obtain a forensic image of all Datamonitor computers Defendant has used and a forensic image of Defendant's Datamonitor e-mail account.

18. Within the Datamonitor Subpoena, Mintel requested both a forensic image of Datamonitor's desktop and/or laptop computers used at any time by Defendant and the forensic image of Defendant's electronic mail account at Datamonitor. *See* Datamonitor Subpoena, attached hereto as "Exhibit 3." Mintel informally served the Datamonitor Subpoena upon opposing counsel, who agreed to accept the informal service. However, Datamonitor has refused to produce the requested images.

19. A party suffers prejudice due to spoliation of evidence when the lost evidence prevents the aggrieved party from using evidence essential to its underlying claim. *Langley v. Union Elec. Co.*, 107 F.3d 510, 514 (7th Cir. 1997). Mintel was relying upon the evidence contained in Defendant's personal computer to establish that Defendant used Mintel's confidential information improperly and interfered with Mintel's business and

clients. As a result of Defendant's spoliation of evidence, and the altered, modified and deleted metadata on Defendant's computer, it is impossible for Mintel to rely upon Defendant's computer to determine the extent of damage caused by Defendant's misappropriation. In fact, countless files have been deliberately deleted and overwritten and, consequently, are no longer recoverable. It follows that, as a result of Defendant's actions, Mintel may no longer rely on evidence from Defendant's computer, and Mintel has clearly been prejudiced by Defendant's spoliation of evidence. Even more concerning is Defendant's blatant and purposeful disregard of the Court's temporary restraining order, which required Defendant to turn over his home computer and refrain from deleting any files from the computer.

20. Based upon Defendant's spoliation of evidence, it is imperative that Mintel obtain all applicable devices and the forensic images requested above in order to determine whether Defendant has used Mintel's confidential information since Defendant's employment with Mintel ended and Defendant's employment with Datamonitor commenced. Again, Defendant is not a credible individual and, therefore, Defendant's testimony that he has not used the information and deleted the misappropriated files shortly after his employment with Mintel ended should not be believed by the Court. If Defendant had nothing to hide, then why did Defendant proceed with altering, deleting and modifying metadata on his personal computer between July 11, 2008 and July 18, 2008? Not only were Defendant's action with regard to his personal computer an egregious attempt to "hide the ball" but also a flagrant discovery violation and violation of the temporary restraining order. Accordingly, Mintel requests that the Court compel Datamonitor to respond to document request numbers 8 and 9 within the Subpoena Rider. More specifically, the Court

should require Datamonitor to provide a forensic image of Defendant's Datamonitor electronic mail account as well as forensic images of all of Datamonitor's computers used by Defendant.

21. Mintel has made the following requests within the Datamonitor Subpoena:

- 5. Produce all documents, including correspondence, that refer to, relate to or otherwise constitute Meesham Neergheen's authorization to work in the United States of America.
- 6. Produce all documents, including correspondence, that refer to Meesham Neergheen's status as an immigrant in the United States of America.
- 7. Produce all documents, including correspondence, that refer to, relate to or constitute the means of Meesham Neergheen's entry into the United States of America.

See Exhibit 3.

22. Datamonitor has similarly refused to produce any responsive documentation, arguing that the documents are not relevant to any of the issues in the pending litigation. However, Defendant is not a United States citizen and, therefore, the requested work authorization documents are relevant to Defendant's start date with Datamonitor.

23. Furthermore, it is important to know whether Defendant has obtained proper authorization to work for Datamonitor. The Seventh Circuit has made clear that "it is a clearly established policy in Illinois to prevent its citizens from violating federal law." *Brandon v. Anesthesia & Pain Management Associates, Ltd.*, 277 F.3d 936, 942 (7th Cir. 2002). Federal law expressly prohibits the employment of aliens who lack proper credentials. *See* 8 U.S.C. § 1324a. Thus, Defendant could not, as a matter of law, be an employee of Datamonitor until he obtained documentation supporting authorization to work within the state. When Defendant was authorized by law to begin work is an important factor as to whether he should be enjoined from remaining employed at Datamonitor.

24. In accordance with Federal Rule of Civil Procedure 37, counsel for Mintel has attempted to resolve this dispute with Defendant's counsel (in the capacity of counsel for Datamonitor). However, all attempts have been unsuccessful and, therefore, court intervention is necessary.

WHEREFORE Plaintiff Mintel International Group, Ltd. respectively requests that this Court grant its Motion to Compel and enter an Order requiring Datamonitor to produce all documentation and things responsive to numbers 5 through 9 within the Subpoena Rider. Mintel further requests any other such relief that the Court may deem just and proper.

Respectfully submitted,

MINTEL INTENTIONAL GROUP, LTD.

By: /s/ Joseph R. Marconi
One of Their Attorneys

Joseph R. Marconi
Victor Pioli
Katherine J. Pronk
JOHNSON & BELL, LTD.
Attorneys for Plaintiff
33 W. Monroe Street, Suite 2700
Chicago, Illinois 60603
(312) 372-0770
Doc. No.: 1920000

CERTIFICATE OF SERVICE

The undersigned hereby certifies that he caused to be served **Plaintiff's Motion to Compel Datamonitor's Compliance with Subpoena** on August 28, 2008 using the CM/ECF System, which will send notification of such filing to the following:

Joel C. Griswold
Jeana R. Lervick
John T. Roache
BELL, BOYD & LLOYD LLP
70 West Madison Street, Suite 3100
Chicago, IL 60602

/s/ Joseph R. Marconi

Joseph R. Marconi – ARDC #01760173
Victor Pioli – ARDC #6256527
Katherine J. Pronk
Johnson & Bell, Ltd.
33 W. Monroe St., Suite 2700
Chicago, IL 60603
312-372-0770

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MINTEL INTERNATIONAL GROUP, LTD., a United Kingdom corporation,	)	
Plaintiff,	)	Civil Action No. 08-cv-3939
v.	)	Hon. Robert M. Dow, Jr.
MEESHAM NEERGHEEN, an individual	)	
Defendant.	)	

AFFIDAVIT OF SCOTT R. JONES

I, Scott R. Jones, due testify from my own personal knowledge as follows:

1. I am employed by Forensicon, Inc. ("Forensicon") as a Senior Forensic Examiner. I also have taught computer forensics at Wilbur Wright College in Chicago, Illinois to both public and private sector students. I possess both a formal education in computer science as well as multiple computer certifications. I have been qualified and have testified as an expert witness in computer forensics before the United States District Court for the Northern District of Illinois, Eastern Division in the matter of Charles A. Krumwiede v. Brighton Associates, L.L.C., and Ismael C. Reyes (Case No. 05 C 3003). Attached as Exhibit A is my curriculum vitae.

2. Forensicon has been retained by counsel for Mintel International Group, LTD. ("Mintel") to provide expert consulting services in the field of computer forensics and electronic discovery.

3. Per the court-approved protocol, an initial Round One set of reports was provided to both parties. The information provided herein is derived from the Round One report set unless otherwise noted. The Round One reports were created for the Item 004 computer ("Item 004"),

EXHIBIT
tabbies
1

which is the computer imaged by Elijah Technologies and reportedly obtained from the Defendant, Meesham Neergheen ("Neergheen"). In addition to the forensic image received from Defense experts, I was also provided a copy of the deposition testimony of Meesham Neergheen as taken on August 13, 2008 ("Neergheen Dep.").

4. Within the Round One reports there is clear evidence of both active and passive efforts to destroy evidence within Item 004. There is also evidence which contradicts Neergheen's deposition testimony of August 13, 2008. The core of evidence destruction and misappropriation activities includes:

- Maintaining custody and continued usage of the Item 004 computer even though he was fully aware that it was the property of Mintel long after departing from Mintel
- Emailing Mintel files to Neergheen's personal Internet-based email account
- The creation and deletion of files and folders, including Windows registry data, well after receiving notice of active litigation
- The deletion of Internet history data for much of the time period prior to July 14, 2008
- The usage of utilities to further obscure dates and times related to files such as antivirus software
- The usage of the Windows defragmentation utility ("defrag") on July 14, 2008 to make deleted file data evidence unrecoverable
- Accessing Microsoft Office and Adobe files after departure from Mintel from both the Internet and from external storage locations as recently as July 17, 2008

5. Neergheen testified that he sent Mintel file data to his personal Internet-based email accounts (Neergheen dep. 42:2-3). Without access to the personal email account(s) used by Neergheen, I cannot verify if any Mintel data still resides therein or if it may have been emailed

to other web-based email accounts. Without examining every computer that Neergheen has used to access his personal web-based email accounts since his departure from Mintel, I may not be able to determine the full extent to which Mintel data has been misappropriated.

6. Defense Expert chain of custody documentation reports that Defense experts received Item 004 from Defense counsel on July 18, 2008. I have seen no written documentation regarding who had physical possession of Item 004 prior to July 18, 2008.

File Entry Activity After July 11, 2008

7. Upon information and belief, active litigation was filed on July 11, 2008. Neergheen was served notice by 6PM that same day (Neergheen Dep. 42:21-22). Neergheen knew that the Item 004 laptop was not his property, but rather, the property of Mintel (Neergheen dep. 27:12-17). Therefore, use of Item 004 thereafter would be inconsistent with a duty to preserve evidence which he had from this approximate time forward.

8. Computers save file data by storing it in segments on a hard drive known as "sectors". The portion of the hard drive that is available and awaiting to receive new file data constitutes "unallocated space". When new file data is created and saved, it is put into those sectors which were formerly unallocated, therefore causing them to become "allocated".

9. By default, when a file is deleted, the computer does not remove the data from the hard drive. Instead, it re-designates those sectors which contain the deleted file data as unallocated space, and those sectors are thereafter available to receive new file data.

10. As long as new data does not overwrite the previously deleted data, it is generally recoverable and available for review. However, the receipt of new file data in a sector causes the

previous file data to become "overwritten". Once the old data has been overwritten, it becomes unrecoverable.

11. The EnCase forensic image of Item 004 reports that over 3,900 file entries were created on or after July 13, 2008. Multiple file entries also report as deleted and having been Last Accessed on or after July 13, 2008. As this is two calendar days after the start of active litigation, Neergheen should not have been using Item 004 and causing data to become deleted. The creation of new file entries has eliinated at least some evidence which I otherwise would have been able to inspect if not for its destruction. As shall be detailed further, the evidence for spoliation within Item 004 goes much deeper than this surface-level review of file activities, but even such a minimal review demonstrates a failure to preserve evidence on the part of Neergheen. Neergheen testified that he did not delete any documents from Item 004 following his receipt of the complaint until the time he surrendered it (Neergheen dep. 48:17–21). Neergheen fails to account for how approximately 98 file entries were deleted following his receipt of the complaint until as recently as July 18, 2008. Some of these file entries report being created as early as May 2008, well before the active litigation was filed, and include Windows system file entries such as restore points and file entries related to the Skype communications tool. Contrary to Neergheen's deposition testimony, file data was deleted from Item 004 well after Neergheen received notice of active litigation.

Neergheen's Level of Expertise

12. Neergheen testified that he received a bachelors degree related to engineering, and that part of that curriculum included electrical and computer engineering (Neergheen dep. 10:11-17). Neergheen also testified that he was educated in computer programming (Neergheen dep. 11:3-

8). Neergheen testified that he began performing database work for Mintel (Neergheen dep. 14:16-19) and further testified that "...it was marketing's role to make sure that contacts were put into the database." (Neergheen dep. 24:5-7) Neergheen concedes that he sent himself Mintel documents via email (Neergheen dep. 42:2–3), so he possesses this computer knowledge as well. Therefore, while the exact level of computer understanding Neergheen possesses is unclear, given his formal education in computer and electrical engineering, and given his several years experience using and learning Mintel's database tools and other computer network resources, and given his admitted understanding of how to transfer Mintel file data via email, I am disinclined to accept at face value Neergheen's deposition testimony that he is "...not a computer savvy person." (Neergheen dep. 12: 10-11) As shall be detailed further herein, information which is not generally accessible to a novice computer user was deleted from the Item 004 computer following July 11, 2008 18:00. It is my opinion that either Neergheen has more computer knowledge than he admits to having, or Neergheen is able to follow documentation and instructions as would be found from websites like "support.microsoft.com", or finally, that there is at least one undisclosed entity who may have aided in the destruction of evidence within the Item 004 laptop computer.

Use of Antivirus Software to Obscure Date and Time Metadata

13. McAfee antivirus software was used on Item 004, and I found that file entries related to the McAfee software within Item 004 reported file activity on July 18, 2008 at 06:46:08, less than 12 hours before Item 004 was forensically preserved. I also found McAfee Antivirus log files reporting updating activity on July 17, 2007. When programs such as antivirus software scan the file entries within a computer, they can alter the time/date metadata for file entries,

thereby obscuring to some degree the patterns of activity that could be found by performing time and date analysis. Such a review looks at the times and dates reported by file entries to locate patterns or trends, and the continued usage of antivirus software up until the date of forensic imaging can obscure previous dates and times of file access. In short, this further destroys evidence related to dates and times which would exist if not for the usage of antivirus software within Item 004. Were the computer turned off and left alone starting on July 11, 2008, as it should have been following receipt of notice of active litigation, the antivirus software would not have been able to alter time and date metadata for any file entries.

14. Table One contains a subset of the Item 004 All Files Present information from within the Round One report production. It reflects Last Access times for a subset of antivirus software file entries.

TABLE ONE

Name	Last Accessed	Full Path
vscan.bof	7/18/2008 6:44:36 AM	MINTELIGROUP_004v611\1393_Meesham_Neerghee n_Sony_PCG-641R_SN_28397627\C\Program Files\McAfee\VirusScan Enterprise\vscan.bof
naisign.dll	7/18/2008 6:44:36 AM	MINTELIGROUP_004v611\1393_Meesham_Neerghee n_Sony_PCG-641R_SN_28397627\C\Program Files\McAfee\Common Framework\naisign.dll
FrameworkService.exe	7/18/2008 6:44:36 AM	MINTELIGROUP_004v611\1393_Meesham_Neerghee n_Sony_PCG-641R_SN_28397627\C\Program Files\McAfee\Common Framework\FrameworkService.exe
graphics.dll	7/18/2008 6:44:36 AM	MINTELIGROUP_004v611\1393_Meesham_Neerghee n_Sony_PCG-641R_SN_28397627\C\Program Files\McAfee\VirusScan Enterprise\graphics.dll
ScriptCI.dll	7/18/2008 6:46:08 AM	MINTELIGROUP_004v611\1393_Meesham_Neerghee n_Sony_PCG-641R_SN_28397627\C\Program Files\McAfee\VirusScan Enterprise\ScriptCI.dll

15. Both active and passive efforts of evidence destruction took place within Item 004. Not only was Item 004 actively used after Neergheen received notice of litigation, causing new file entries to be created and thereby overwriting unallocated space, but Neergheen also failed to stop automated system utilities from running that would destroy and/or alter evidence as recently as the very day in which Item 004 was forensically preserved. Stopping any automated processes

from running was as simple as removing both the battery and power cord from the laptop, and very little technical knowledge would be required to do this. Certainly a person having a formal education in computer and electrical engineering (Neergheen dep. 10:11-17) could accomplish this task if s/he so desired and were directed to do so by counsel.

Spoliation Noted Within Item 004 Internet History

16. A common convention with Microsoft Windows is that a user's name is reflected by their user profile. For example, within Item 004, the user profile "Meesham Neergheen" is logically tied to the Defendant, and was likely used by the Defendant within Item 004. It is possible for persons to use profiles that do not clearly denote their actual name. There are multiple user profiles which do appear to denote the names of persons who have used the Item 004 computer. Upon information and belief, many of the names reflected by the user profiles within Item 004 are current or former employees of Mintel.

17. Neergheen testified that from July 11, 2008 at 18:00, only he and his counsel had access to his username and password information used within Item 004 (Neergheen dep. 93:22 – 94:4), and only he and his counsel had access to Item 004 since that time (Neergheen dep. 143:16-19). Activities reflecting Neergheen's user profile after this time logically were caused by those who possessed this requisite information, or others to whom were granted physical access to Item 004 after the username and password information was entered.

18. Item 004 Internet history data reports that on July 17, 2008, the user profile "Meesham Neergheen" visited the website "http://support.microsoft.com" around 6:41 AM. Neergheen's profile searched Microsoft's website for information related to deleting file data as is detailed

within Tables Two and Three. Neergheen admitted to visiting this website during his deposition testimony (Neergheen dep. 145:12-16).

19. Table Two contains a subset of the data within the original Item 004 Internet History information previously released to all parties per the agreed protocol.

TABLE TWO

ID	Profile Name	Url Name	Last Accessed
2368	meesham neergheen	http://support.microsoft.com/	7/17/2008 6:41:17 AM
2315		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20d	7/17/2008 6:41:37 AM
2311		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do	7/17/2008 6:41:38 AM
2313		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do%20i	7/17/2008 6:41:38 AM
2308		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do%20i%20a	7/17/2008 6:41:40 AM
2305		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do%20i%20acess	7/17/2008 6:41:41 AM
2300		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do%20i%20aces	7/17/2008 6:41:42 AM
2301		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do%20i%20ace	7/17/2008 6:41:42 AM
2302		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do%20i%20ac	7/17/2008 6:41:42 AM
2294		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do%20i%20acc	7/17/2008 6:41:43 AM
2296		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do%20i%20access	7/17/2008 6:41:43 AM
2297		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=how%20do%20i%20acce	7/17/2008 6:41:43 AM
2293		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=dele	7/17/2008 6:41:50 AM
2291		http://autocomplete.support.microsoft.com/ACSearchSuggest.aspx?lcid=1033&query=deleted	7/17/2008 6:41:50 AM

20. Within Table Two, the column "Url Name" reports the web address that was visited at the reported time of last access. For most of the rows in Table Two, the information reports that Microsoft's support website was queried for specific information related to accessing and/or deleting information from within the Item 004 computer. Neergheen admits to visiting this website and looking for information (Neergheen dep. 145:12-16). Following the "query=" text in this column is displayed the text that Neergheen typed into Microsoft's search bar while he

visited Microsoft's support website. For a simplified view of the query text, see Table Three following.

TABLE THREE

ID	Query Text Clarified
2368	http://support.microsoft.com/
2315	query=how d
2311	query=how do
2313	query=how do i
2308	query=how do i a
2305	query=how do i acess
2300	query=how do i aces
2301	query=how do i ace
2302	query=how do i ac
2294	query=how do i acc
2296	query=how do i access
2297	query=how do i acce
2293	query=dele
2291	query=deleted

NOTE: "ID" aligns both to TABLE TWO and the original Item 004 Internet History report already produced to the parties.

21. In order to obtain a better understanding of the information that Neergheen saw when he typed the above queries into Microsoft's support website, I entered the same queries that Neergheen entered on July 17, 2008 into my Internet Explorer browser. Exhibit B contains partial screenshots showing what information I found when I approximated his actions.

22. When I visited the website "http://support.microsoft.com" and typed in the same queries that Neergheen entered on July 17, 2008, I found references to information on how to delete data from a Microsoft Windows computer. As displayed within the Exhibit B screenshot using query data from ID 2293, the topics listed include the deletion of registry keys, partitions, files and folders, temporary internet files and more. As has already been mentioned, and shall be detailed further herein, I found deleted registry data and other Windows operating system artifacts,

deleted Internet history data, and deleted file entries of various types. The Microsoft support information that Neergheen's profile actively sought closely aligns to the evidence destruction I found within Item 004.

23. Item 004 was likely used on July 17, 2008 to obtain information from Microsoft on how to delete information from within a computer running a Microsoft operating system. As litigation was filed on July 11, 2008, and since Neergheen had legal representation since at least July 15, 2008, Neergheen should not have been using the computer and thereby destroying evidence on July 17, 2008. Simply powering up a computer can cause file data to be created and/or altered, which destroys evidence that would otherwise have been available for review had Item 004 not been in use. What is further disturbing is that Item 004 appears to have been used to search for information about how to delete data from within Item 004. Continued usage of Item 004 after notice of active litigation is incompatible with good-faith efforts to preserve evidence, and searching for information about how to delete data from Item 004 suggests the intent to destroy evidence.

24. Without inspecting the forensic image for the unproduced Dell desktop computer that Neergheen testified to having used for several months (Neergheen dep. 29:8-30:7), or other computers which he has used since his departure from Mintel, I will not be able to determine if Neergheen performed similar searches on those computers for information related to deleting file data from a computer as I believe he did using Item 004.

Missing Internet History Data

25. The user profile Meesham Neergheen is missing Internet history data which would report activity from the time period prior to his termination from Mintel until just after the time when

active litigation was filed. The gaps in daily Internet history appear to be selective in that there are existing daily records for specific dates with gaps in between. Alternatively, there does not appear to be weekly Internet history data for Neergheen's profile for the time period between the earliest known daily Internet history date, January 23, 2008, and June 23, 2008, which strongly suggests that the data was purged. Finally, one deleted file entry related to daily Internet history from the period following Neergheen's termination from Mintel was found, which further supports that the time period following Neergheen's departure from Mintel until about July 14, 2008 was selected for deletion.

26. The Windows operating system employed by Item 004 creates file entries for both weekly and daily Internet history data. The names of these file entries generally denote the time periods of data which they store. The file entry's name can be segmented for better understanding as follows:

"MSHist01" + [START DATE] + [END DATE]

For example, the file entry "MSHist012008071420080715" would contain daily Internet usage information for July 14, 2008 to July 15, 2008. There are also gaps in daily internet history for the time periods between February 27, 2008 to May 3, 2008 and January 24, 2008 to February 26, 2008. The Internet history data for May 3, 2008 to May 4, 2008 was also deleted, but did not report as being overwritten. Were it deleted and overwritten, the missing Internet history data would have spanned the time period from February 27, 2008 to July 14, 2008.

27. Table Four contains a subset of data derived from the Item 004 All Files reports provided to all parties according to the protocol. It reflects Internet history data only related to the user profile "Meesham Neergheen".

TABLE FOUR

Daily	Weekly
MSHist012008012320080124	Where is the missing Weekly Internet Data from 2008/01/23 - 2008/06/23?
GAP	
MSHist012008022620080227	
GAP	
MSHist012008050320080504**	MSHist012008062320080630
GAP - covers time before & right after notification	MSHist012008063020080707
MSHist012008071420080715	MSHist012008070720080714
MSHist012008071520080716	Device likely imaged prior to creation of further weekly history
MSHist012008071620080717	
MSHist012008071720080718	
MSHist012008071820080719	
** NOTE: Reports as Deleted, but not as overwritten	

28. Note the missing time periods for daily Internet history information in Table Four. The Internet history data for the time period of May 3, 2008 to May 4, 2008 reported as having been deleted, but not overwritten. Therefore, it appears as though somebody targeted the Neergheen Internet history data covering the time period following Neergheen's reported departure from Mintel on April 30, 2008 until July 14, 2008 for deletion. If there is existing daily Internet history data from January 2008, there should also be the weekly corollary data from January 2008 forward. The daily information appears to have been selectively deleted while the weekly information prior to June 23, 2008 was deleted en masse. In misappropriation cases, it is common for a user to delete Internet history data which would reflect notable actions such as the continued access and usage of emailed file data following their departure from one company and after beginning employment with another.

Spoliation Noted Within The Registry – Reported By The Item 004 USBSTOR Report

29. The Item 004 USBSTOR report contains further evidence of data deletion from the Item 004 computer. This particular Round One report contains Windows Registry information related

to storage devices that have been connected to Item 004 via the Universal Serial Bus ("USB"). As such, it would normally contain targets for further discovery because the devices listed therein are regularly involved with cases of data misappropriation or trade secret theft. These devices are typically used to both transfer and/or store file data.

30. The non-savvy computer user likely is unable to access the Windows registry or even specifically target a single portion of the Windows registry for deletion. Such an advanced act of data deletion denotes elevated computer knowledge on the part of the person who carried out the action. Neergheen testified that only he and his counsel had access to Item 004 following July 11, 2008 18:00 (Neergheen dep. 143:16-19). An advanced action such as accessing and then deleting portions of the Windows registry contradicts Neergheen's testimony that he is not "computer savvy" (Neergheen dep. 12: 10-11). Alternatively, it suggests that Neergheen had help which to date he has not disclosed or that he was able to follow technical information obtained from the Internet on how to access and delete Windows registry data (see Exhibit B).

31. In reviewing the USBSTOR information for Item 004, it is highly notable that on July 17, 2008, there are two USB storage devices which not only report having their settings updated, thereby supporting connection to Item 004, but also report as being deleted sometime thereafter. Table Five contains a subset of the Item 004 USBSTOR data previously provided to all parties per the protocol. Neergheen admits to possessing and using two USB storage devices (Neergheen dep. 96:22–97:9).

32. Neergheen admitted to visiting Microsoft's support website and performing Internet searches at approximately 6:41 AM on July 17, 2008 (Neergheen dep. 145:12-16), where it appears that he searched for technical instructions from Microsoft's website about how to access and/or delete data from Item 004. Sometime after 13:15, multiple entries within the Windows

USBSTOR registry report as being both last written and also deleted. In order for the file entries to be last written, they must have existed at the time they were last written. Therefore, they were deleted sometime after their reported last written time.

33. I have inspected many Windows computers which contained data within their USBSTOR registry settings. Many of these computers had data therein that were years old and yet not deleted. The Windows operating system itself would not need to delete the USBSTOR information in order to function optimally, and to my knowledge, there is no system-performance-based reason for this information to have been deleted from Item 004. Given the fact that it occurred after litigation was filed and notice served to Neergheen, and also given its proximity to Neergheen's profile searching Microsoft's website for technical instructions on how to access and delete data, it is my opinion that this activity was an attempt at destroying evidence regarding devices by which Neergheen transferred, stored, and/or used Mintel file data (Neergheen dep. 96:19-21). Only after the Defense expert turns over the forensic images for the devices listed within the Item 004 USBSTOR report will I be able to review them and determine if they contain Mintel trade secrets or intellectual property, as well as determine if spoliation also occurred within those devices.

34. If one filters the Item 004 USBSTOR report from within the Round One reports such that it only shows entries that report as "Deleted, Registry Entry", they will see multiple pages of printed output reflecting hundreds of file entries and multiple devices that may contain misappropriated data or trade secrets. If there were no Mintel trade secret or intellectual property therein, there would be no need to purge the data reporting the existence of the devices well after the defendant had a duty to preserve evidence. Such purging is consistent with efforts to obscure user activities and eliminate evidence from within the Item 004 computer.

35. The fact that Windows registry entries relating to USB storage devices which were attached to Item 004 on July 17, 2008 were deleted sometime after Neergheen searched Microsoft's website for information related to accessing and/or deleting data strongly suggests that the deletion of the USBSTOR Windows registry data was deliberate.

36. The root folder of Neergheen's profile reports a creation date of June 14, 2006. Therefore, if Neergheen used Item 004 after this time period, USB storage devices connected on or after this date could have been used to misappropriate Mintel data other than what Neergheen has already admitted to taking (Neergheen dep. 42:2-3 and 45:10-15).

37. Table Five contains a subset of the Item 004 USBSTOR report data. It denotes devices named "USB007 mini-USB2BU", "USB Flash_Disk" (named twice but with different serial numbers), "Apple iPod", and "LEXAR JD_EXPRESSION".

TABLE FIVE

ID #	Description	Is Deleted	Last Written	Full Path
2	Folder, Deleted, Registry Entry	Yes	7/17/2008 1:46:55 PM	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\system32\config\system\NTRegistry\$$$PROTO.HIV\ControlSet001\Enum\USBSTOR\Disk&Ven_USB007&Prod_mini-USB2BU&Rev_0.00\000000000000A9&0
11	Folder, Deleted, Registry Entry	Yes	7/17/2008 1:15:18 PM	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\system32\config\system\NTRegistry\$$$PROTO.HIV\ControlSet001\Enum\USBSTOR\Disk&Ven_USB&Prod_Flash_Disk&Rev_5.00\2007062000000072&0
21	Folder, Deleted, Registry Entry	Yes	7/15/2008 3:54:43 PM	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\system32\config\system\NTRegistry\$$$PROTO.HIV\ControlSet001\Enum\USBSTOR\Disk&Ven_USB&Prod_Flash_Disk&Rev_5.00\2007062800000616&0
28	Folder, Deleted, Registry Entry	Yes	7/8/2008 9:11:23 PM	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\system32\config\system\NTRegistry\$$$PROTO.HIV\ControlSet001\Enum\USBSTOR\Disk&Ven_Apple&Prod_iPod&Rev_1.62\000A27001BB74888&0
63	Folder, Deleted, Registry Entry	Yes	11/24/2007 10:49:55 AM	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\system32\config\system\NTRegistry\$$$PROTO.HIV\ControlSet001\Enum\USBSTOR\Disk&Ven_LEXAR&Prod_JD_EXPRESSION&Rev_1.00\302AC2070729262&0

38. Contrary to Neergheen's testimony that he only possessed and connected two USB storage devices to Item 004 (Neergheen dep. 96:3-97:9), the deleted file entries related to the Windows USBSTOR registry show that in the time since June 14, 2006, at least five USB storage devices have been connected. Furthermore, four USB devices reporting unique serial numbers have been connected since July 8, 2008. It is unclear which two of the five devices Neergheen testified to connecting to Item 004 or why Neergheen did not disclose all four storage devices connected in July 2008. Only Neergheen can explain the omissions in his testimony.

39. I do not know if the devices listed within Table Five were also preserved forensically so that they can be examined. Once Defense experts do so, I can review the forensic images to better determine if evidence was destroyed therein as has occurred in Item 004. Furthermore, were I to receive forensic images for other computers to which these devices have been connected, I could compare the forensic images with Item 004 to confirm similarities of USB device connectivity and discover the extent to which Mintel data migrated to any other locations. Neergheen testified to having and using only two devices, but the evidence reports four distinct serial numbers for devices connected in July 2008. My forensics training and professional experience leads me to believe that such omissions are consistent with efforts to conceal the existence of two or three USB storage devices which likely contained Mintel trade secret file data and were likely connected to other computers since Neergheen's departure from Mintel.

Link Files Show Access of File Data Within USB Storage Devices & the Internet

40. Within the Round One reports there is a report entitled "Item004_LinkFileReport". This report contains information related to link files found within Item 004. Link files are simply shortcuts or pointers to other files. For example, when someone opens a Microsoft Word file that

they emailed and/or stored within a web-based email account, that action creates one or more link files on their Windows computer. Although they may not have saved the file locally to their computer, one or more shortcuts to that file which contain some of the file metadata from the original file would typically have been created. By examining the data within link files, one can determine much about the files someone has accessed even if they have taken steps to delete the original file. It is common in misappropriation cases that a person deletes an original file, but fails to delete all link file references to file data.

41. In examining the link files within Item 004, I found evidence that Neergheen accessed file data stored within removable storage devices as recently as July 17, 2008 around 13:50. This closely aligns to the USB storage device information reported formerly within Table Five, which reports that on July 17, 2008 after 13:15, Neergheen connected at least two USB storage devices. At around 13:50, Neergheen accessed an Adobe PDF file named "show_temp 1.pdf" from a USB storage device.

42. I also found information that establishes that following Neergheen's departure from Mintel, multiple Microsoft Office type files were accessed via the Internet on various dates and times. Link file creation generally denotes file access because accessing a file is what frequently causes the link file to be created. The link files within Item 004 suggest that beyond checking email for new messages, the Internet was used to access actual file data of like kinds to the types of file data which Neergheen admits to having sent himself via email (Neergheen dep. 42:2-3).

43. Table Six contains a subset of the Item 004 link files data. Table Six reports Internet usage data which occurred within the time period of the purged Internet history file entries (see Table Four). This further suggests that the deletion of the Internet history data prior to July 14,

2008 occurred in order to conceal the usage of common file types, such as the Mintel file data which Neergheen admitted to emailing to his personal email (Neergheen dep. 42:2-3).

TABLE SIX

ID	Link File	Created Date	Modified Date	Last Accessed	Drive Type	Serial	Base Path
29	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\Documents and Settings\Meesham Neergheen\Application Data\Microsoft\Office\Recent\Datamonitor Document.LNK	3/2/2008 8:16:22 PM	3/2/2008 8:16:26 PM	3/02/2008	Removable	00 0B 5C DF	D:\Datamonitor Document.doc
3	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\Documents and Settings\Meesham Neergheen\Recent\show_temp 1 .lnk	7/17/2008 1:50:12 PM	7/17/2008 1:50:14 PM	7/17/2008	Removable	B8 72 42 FD	D:\show_temp 1 .pdf
8	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\Documents and Settings\Meesham Neergheen\Application Data\Microsoft\Office\Recent\Intro to FS 20080327[1].LNK	5/23/2008 10:18:40 AM	5/23/2008 10:19:03 AM	5/23/2008 10:19:07 AM	Fixed	5C 71 5A EF	C:\Documents and Settings\Meesham Neergheen\Local Settings\Temporary Internet Files\Content.IE5\47DBAM3P\ Intro to FS 20080327[1].ppt
9	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\Documents and Settings\Meesham Neergheen\Application Data\Microsoft\Office\Recent\Meesham Neergheen[1].LNK	5/7/2008 1:31:43 PM	5/7/2008 1:31:46 PM	5/7/2008 1:31:47 PM	Fixed	5C 71 5A EF	C:\Documents and Settings\Meesham Neergheen\Local Settings\Temporary Internet Files\Content.IE5\S9EN0P23\ Meesham Neergheen[1].doc
13	MINTELIGROUP_v67_004\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\Documents and Settings\Meesham Neergheen\Application Data\Microsoft\Office\Recent\Meesham Neergheen - Confidentiality letter[1].LNK	5/7/2008 1:23:02 PM	5/7/2008 1:23:13 PM	5/7/2008 1:23:19 PM	Fixed	5C 71 5A EF	C:\Documents and Settings\Meesham Neergheen\Local Settings\Temporary Internet Files\Content.IE5\APST69CJ\ Meesham Neergheen - Confidentiality letter[1].doc

Spoliation Noted Within The Item 004 Windows Prefetch File Entries

44. Windows caches information in multiple places throughout the operating system. One of the places that Windows stores information for programs run on the computer - executable files (.EXE) - is commonly known as the Windows Prefetch ("prefetch") Folder. When an .EXE file is run, Windows often creates a file entry within the prefetch which stores information related to the use of the .EXE file. Therefore the creation date of the prefetch file entry is a strong indicator that a particular executable file (.EXE) was used to run a program on a given date.

45. Besides the creation date of a prefetch file entry, the date that the prefetch file entry reports last written is another indicator of the most recent time that an .EXE file was run. This is because Windows updates the information within the prefetch file entry to catalog the number of times it has been run since the creation of the prefetch entry. By considering both the creation and last written dates for a prefetch entry, one can surmise the earliest known and most recent usage of an .EXE file to run a program.

46. The Item 004 prefetch file entries report the use of the Windows defragmentation utility ("defrag"), on or about July 14, 2008 at 18:39. This usage was well after Neergheen received notice of the active litigation on July 11, 2008 (Neergheen dep. 42:21-22). The use of the defrag utility after deleting file data is a commonly-employed means of rendering deleted file data forever unrecoverable in the file data's original native format, if at all.

47. As noted previously in paragraph 8, file data is stored in sectors, and these sectors of data related to the same file can become scattered across a hard drive or storage medium. This causes the computer to operate more slowly when accessing that data. The defrag utility is a tool that can improve system performance by reordering the scattered file data into a contiguous group of sectors, thereby allowing for faster read times by the computer. The down side to this process is that in moving the sectors of file data about the hard drive or storage medium, existing file data often overwrites previously-deleted file data which was recoverable prior to the defrag process. Once a deleted file is overwritten with new data, it is generally no longer recoverable or available for review in its original native format, if at all.

48. I found no indication that defrag was run as part of an automated system process, which suggests that someone ran this utility deliberately on July 14, 2008.

49. In addition to the usage of defrag to destroy evidence within Item 004, other prefetch file entries report creation and/or being last written on July 17, 2008. This further file entry creation necessarily overwrites previously unallocated space which contained evidence. If not for the file creation activities which destroyed evidence within Item 004, this previously-deleted file data would have been available for review. The prefetch file entries report file activity as recently as July 18, 2008 around 07:23:27.

50. The prefetch file entries alone show that contrary to Neergheen's testimony that after he received the complaint he only used the Internet (Neergheen dep. 48:22-49:2), Neergheen used both the Skype utility around 17:58 and defrag around 18:39 on July 14, 2008. Furthermore, prefetch file entries report that a Skype installation .EXE file was run on May 1, 2008 around 16:11. This seems to contradict Neergheen's testimony that he used Skype while employed for Mintel, "…but I don't use it now." (Neergheen dep. 98:17-18) Neergheen testified that Skype "allows you to communicate with other colleagues within a company and also anywhere around the world." (Neergheen dep. 98:13-15). Neergheen clearly used Skype after his departure from Mintel on April 30, 2008. As Skype uses the Internet, this further implicates that the deletion of Internet history information prior to July 14, 2008 is even more suspicious. It also notes another layer of "computer savvy" possessed by Neergheen.

51. Table Seven contains a subset of the Windows Prefetch data from within the Item 004 All Files Present report that was contained within the Round One production set. In addition to the admitted usage of the Internet, Table Seven reports the use of multiple applications, such as Skype, defrag, Microsoft Calculator, Adobe Acrobat Reader, Microsoft PowerPoint, McAfee Antivirus software, and more. This usage is in direct contradiction to Neergheen's testimony that

aside from using the Internet, he did not run any other programs on Item 004 (Neergheen dep. 48:22-49:2).

TABLE SEVEN

Name	File Created	Last Written	Full Path
SKYPE.EXE-1C7D242A.pf	5/1/2008 4:12:36 PM	7/14/2008 5:58:47 PM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\SKYPE.EXE-1C7D242A.pf
DEFRAG.EXE-273F131E.pf	4/2/2007 9:46:38 AM	7/14/2008 6:39:05 PM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\DEFRAG.EXE-273F131E.pf
DFRGNTFS.EXE-269967DF.pf	4/2/2007 9:46:38 AM	7/14/2008 6:39:05 PM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\DFRGNTFS.EXE-269967DF.pf
CALC.EXE-02CD573A.pf	1/1/2008 8:12:52 PM	7/17/2008 11:13:03 AM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\CALC.EXE-02CD573A.pf
ACRORD32.EXE-13285B88.pf	12/7/2007 10:15:11 PM	7/17/2008 1:07:30 PM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\ACRORD32.EXE-13285B88.pf
POWERPNT.EXE-17CE3F4E.pf	1/25/2008 8:08:08 PM	7/17/2008 1:14:38 PM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\POWERPNT.EXE-17CE3F4E.pf
ACRORD32INFO.EXE-013EA364.pf	2/2/2008 9:00:22 PM	7/17/2008 1:46:09 PM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\ACRORD32INFO.EXE-013EA364.pf
MCUPDATE.EXE-1D0E3EC0.pf	9/14/2007 10:03:27 AM	7/17/2008 5:31:14 PM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\MCUPDATE.EXE-1D0E3EC0.pf
USERINIT.EXE-30B18140.pf	4/21/2006 9:12:21 AM	7/18/2008 6:44:49 AM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\USERINIT.EXE-30B18140.pf
WUAUCLT.EXE-399A8E72.pf	4/21/2006 9:12:37 AM	7/18/2008 6:44:50 AM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\WUAUCLT.EXE-399A8E72.pf
IEXPLORE.EXE-27122324.pf	10/5/2007 9:01:17 AM	7/18/2008 6:46:18 AM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf
LOGON.SCR-151EFAEA.pf	4/21/2006 11:58:19 AM	7/18/2008 7:23:27 AM	MINTELIGROUP_004v611\1393_Meesham_Neergheen_Sony_PCG-641R_SN_28397627\C\WINDOWS\Prefetch\LOGON.SCR-151EFAEA.pf

Conclusion

52. Neergheen confirmed that the allegations in the complaint were true (Neergheen dep. 45:10-15). Neergheen concedes that he maintained possession of Mintel's property after he was no longer employed by Mintel even though he knew the Item 004 laptop to be Mintel's property (Neergheen dep. 26:23-27:17). Neergheen testified to being served notice of the active litigation on July 11, 2008 (Neergheen dep. 42:21-22). His continued usage of Item 004 was inconsistent with efforts to preserve evidence within Item 004. Simply using the computer will cause new data to be created which will overwrite previously-deleted file data and thereby ruin evidence within a computer.

53. Given that Neergheen testified that the allegations in the complaint were true (Neergheen dep. 45:10-15) it is questionable why Neergheen took such advanced steps to delete evidence from Item 004. From the pieces of evidence and testimony that I have seen thus far, it is clear that Neergheen tried to hide the details of his activities from the time period around his departure from Mintel until around July 14, 2008, after he was employed by his present employer and after he was served notice of litigation.

54. Internet history data for Neergheen's profile for specific time periods before July 14, 2008 were deleted. With the exception of a single deleted file entry, the daily Internet history file entries were purged from Item 004 for the time period of February 27, 2008 until July 14, 2008. The Item004_LinkFileReport data within the Round One reports show that Neergheen accessed common file data types such as Microsoft Word (DOC) and Microsoft PowerPoint (PPT) files via the Internet during the time period covered by the purged Internet history file entries. I believe that Neergheen tried to hide his access of common business file data types from the Internet because he likely accessed the Mintel file data that he sent to his personal email after he

began working at his current job. Neergheen concedes that on Friday, April 25, 2008, after he already accepted the employment offer with his present employer, he sent Mintel file data to his personal email (Neergheen dep. 137:21-138:6). People who misappropriate company file data often take file data that they think will benefit them in some way at their new job by emailing it to a personal email account.

55. Neergheen testified to visiting Microsoft's support website and searching it for information on July 17, 2008 (Neergheen dep. 145:12-16). The available Item 004 Internet history data for Neergheen's profile supports that he searched a Microsoft website for information related to data deletion. Subsequent to that searching activity on July 17, 2008, sometime after 13:46, portions of the Windows registry were deleted which contained evidence of attached storage devices which are targets for further discovery. Neergheen's actions suggest elevated computer knowledge and/or the ability to follow directions when desired. Alternatively, Neergheen may have also had assistance in deleting evidence such as the Windows registry data.

56. With regard to USB storage devices, Neergheen's testimony was that he only owns two devices (Neergheen dep. 96:22-97:2) and that he has only used two USB storage devices (Neergheen dep. 97:3-9). The evidence within Item 004 reports that in July 2008, at least four USB storage devices with unique serial numbers were attached to Item 004. Neergheen may not own them all, but if only he or his counsel had access to Item 004 after July 11, 2008 (Neergheen dep. 143:16-19), it is imperative to identify who owns or possesses the devices now, and who used them during July 2008.

57. Since Neergheen testified that he has used flash drives to transport Mintel data (Neergheen dep. 96:19-97:9), I would need to examine the forensic images for each of the USB storage devices listed within Table Five. After Defense experts create the forensic images as they

did for Item 004, I will be able to review the devices and determine if they contained Mintel file data at the time of imaging, or if steps were taken to destroy evidence from within the USB storage devices as has occurred within Item 004.

58. I do not know if or when Neergheen's counsel instructed him that he had a duty to preserve evidence and he should stop using Item 004. The evidence reflects that Item 004 was in use up to July 18, 2008, the very day it was forensically imaged, and that both active and passive steps were employed to destroy evidence from the Item 004 laptop computer.

Further Affiant Saith Not.

Scott R. Jones, EnCE, CompTIA A+
Paraben Certified PDA Examiner

Subscribed and Sworn to before me
this 21st day of August, 2008.

NOTARY PUBLIC

OFFICIAL SEAL
LEE M NEUBECKER
NOTARY PUBLIC - STATE OF ILLINOIS
MY COMMISSION EXPIRES:05/18/09

EXHIBIT A

Forensicon
Computer Forensics Specialists

Internal Investigations ◆ Trade Secrets ◆ Employment Litigation

EXHIBIT A CURRICULUM VITAE EXHIBIT A

Scott Jones

Scott Jones is a Senior Forensic Examiner for Forensicon, Inc. Mr. Jones provides consulting services in the areas of computer forensics, electronic discovery, data recovery, expert witness testimony and litigation support for clients spanning many areas of industry, from small businesses to large corporations. Mr. Jones has worked in support of both Plaintiff and Defense counsels, and has additionally served in a third-party neutral expert capacity for civil litigation cases. Mr. Jones has testified as an expert witness in computer forensics before the United States District Court for the Northern District of Illinois, Eastern Division, and has offered written and verbal testimony for the Circuit Court of Cook County, Illinois, before the Financial Industry Regulatory Authority ("FINRA", formerly "NASD") and the Occupational Safety and Health Administration ("OSHA").

Mr. Jones possesses critical computer and forensics certifications from organizations such as CompTIA, Guidance Software, and Paraben Software. He possesses the CompTIA A+ certification, Guidance Software's EnCE (EnCase Certified Examiner) designation, and has completed requirements for Paraben Software Corporation's Certified PDA Examiner designation.

In addition to Mr. Jones's various certifications, his professional experience in computer forensics and computer science has enabled him to be accepted as an instructor at Wilbur Wright College in Chicago, Illinois. Mr. Jones has taught computer forensics for the Computer Security & Forensic Investigations program to students from both civilian and government/law enforcement populations.

On multiple occasions, Mr. Jones has been consulted by local media outlets due to his technical understanding and professional reputation. He has been interviewed both WGN-TV and WCIU-TV.

Prior to teaching computer forensics at Wright College, and also prior to working for Forensicon, Inc., Mr. Jones worked for Sprint PCS. While at Sprint PCS, Mr. Jones provided technical support for customers needing to integrate Sprint PCS cellular devices and services with their existing computer(s). Mr. Jones also initiated fraud investigations based upon client activities and also assisted with both device repair and inventory control procedures.

Prior to Sprint PCS, Mr. Jones was employed as a Senior Computer Repair Technician for a publicly-traded retail chain. His years of experience in computer repair and technical support, along with his ability to train others helped him attain the "Tech Bench MVP" award in November 2001.

Mr. Jones graduated *cum laude* from DeVry Institute of Technology with a Bachelor of Science in Information Technology. Mr. Jones has also earned a Bachelor of Science of Administrative Management degree with a Minor in Music from Eastern Illinois University. He is presently pursuing a Masters of Science in Information Technology Law degree from The John Marshall Law School in Chicago, Illinois.

EXHIBIT A

Forensicon

AFFIDAVITS - DEPOSITIONS - EXPERT TESTIMONY - CONSULTING

Civil Action No. 05 C 3003
Charles A. Krumwiede v. Brighton Associates, LLC & Ismael Reyes
United States District Court
Northern District of Illinois, Eastern Division
cited at 2006 WL 1308629 (N. Dist. Ill. 05 C 3003), 2006 U.S. Dist. LEXIS 70535

Civil Action No. 06 C 2709
Valuepart, Inc. v. Brett Clemens, Shannon Murphy, and ITR North America
United States District Court
Northern District of Illinois, Eastern Division
Online reference at http://www.duanemorris.com/attorneys/johntschriver.html

Civil Action No. 04 CV 1873
S.C. Johnson & Son, Inc. v. Milton E Morris, et al.
Circuit Court of Racine County
Racine, Wisconsin

Civil Action No. 03 C 8708
Patrick Mudron v. Brown & Brown, Inc.
United States District Court
Northern District of Illinois, Eastern Division

Civil Action No. 03 C 4769
Lorillard Tobacco Co., et al. v.Canstar (USA) Inc, et al.
United States District Court
Northern District of Illinois, Eastern Division

Civil Action No. 07 CV 001679
Terrence O'Malley v. Village of Oak Brook, et al.
United States District Court
Northern District of Illinois, Eastern Division

Civil Action No. 05 L 50500
PCS Administration (USA), Inc. v. Karen Bishop
Circuit Court Of Cook County, Illinois
County Department, Law Division

Civil Action No. 05 CH 289
The Agency, Inc, d/b/a The Agency Staffing v. Janet Grove
Circuit Court of the 19th Judicial Circuit
McHenry County, Illinois
County Department, Chancery Division

EXHIBIT A

Forensicon

PROFESSIONAL DEVELOPMENT

- **EnCase Certified Examiner** (EnCE), Guidance Software, Inc. Obtained February 2005
- **Certified PDA Examiner**, Paraben Corporation, Obtained June 2005
- **CompTIA A+ Certified Professional**, Validation Date: 11/6/2004, ID No. COMP001003247176
- **Associate Member**, Association of Certified Fraud Examiners, Member No. 139286
- **EnCase & Vericept Corporation Seminar,** Implementing an Effective Incident Management System, October 28, 2005 – Oakbrook, Illinois
- **EnCase v5 Briefings Seminar**, April 26, 2005 – Chicago, Illinois, CPE Credits: 4
- **Intermediate Computer Forensics**, May 17-19, 2004 – RCFL, AccessData Corporation – 24 Hours classroom instruction, Chicago, Illinois
- **EnCase Intermediate Analysis & Reporting**, July 30, 2004 – Sterling, Virginia, CPE Credits: 32
- **PDA Seizure & Analysis**, Paraben Corporation – Two days of classroom instruction, June 21-22, 2005, Chicago, Illinois
- **EnCase Incident Response, Forensic Analysis & Discovery**, April 16, 2004 – Sterling, Virginia, CPE Credits: 40

FORMAL EDUCATION

- **Masters of Science in Information Technology Law**, GPA: 3.83/4.0, John Marshall Law School, Chicago, Illinois, In process as of Spring 2007
- **Bachelor of Science in Information Technology**, GPA: 3.67/4.0, Cum Laude & Dean's List, DeVry Institute of Technology, Tinley Park, Illinois, Graduated March 2002
- **Bachelor of Science of Administrative Management**, Music Violin, Minor, Eastern Illinois University Charleston, Illinois, Graduated May 1995

PROFESSIONAL EXPERIENCE

FORENSICON, INC. - Chicago, Illinois (3/04 – Present)
Senior Forensic Examiner

- Perform forensic investigations & analysis of client electronic media including hard drives, floppy disks, CDs/DVDs, & other forms of electronic media. Analysis performed with software tools such as EnCase, FTK, Paraben Device Seizure, & others.
- Train Associate Examiners and support staff as needed
- Create expert written reports for both active litigation and internal investigations.
- Research new technologies & products for use in forensic electronic investigations.
- Work with clients to review discovery requests, case strategies, and design solutions to meet case-specific requirements.
- Participate in & attend professional training classes, seminars, & conferences related to computer forensics & litigation support.
- Promoted to Senior Forensic Examiner in April 2005

WILBUR WRIGHT COLLEGE - Chicago, Illinois (8/05 – 12/06)
Adjunct Instructor, Computer Security & Forensic Investigation Program

- Taught computer forensics to both law enforcement/government and civilian students
- Created & modified curriculum, class assignments, lab projects & lectures as needed
- Assisted with student workshops related to Computer Security & Forensic Investigations

SPRINT PCS – Bolingbrook, Illinois & Downers Grove, Illinois (11/02 to 3/04)

Inventory Support Specialist – Downers Grove, Illinois (11/03 to 3/04)

- Oversaw all aspects of inventory control for retail location including shipping & receiving, physical inventory & store audits, & reporting for Downers Grove Store # 899.
- Reporting included weekly & monthly semi-automated reports using RMS Back Office & Sprint-proprietary systems.
- Researched discrepancies & report results to corporate audit staff.
- Served as on-site technician & technical systems contact for customer & store phone & computer troubleshooting needs.

Level III Tier I Data Specialist – Bolingbrook, Illinois (11/02 – 11/03)

- Provided over-the-phone troubleshooting, programming, & debugging services for clients using Sprint PCS handsets & wireless internet connectivity devices for laptop computers, personal digital assistants, cell phones & other specialty devices.
- Assisted customers with the installation & configuration of Sprint & Sprint-approved software for Windows versions 95 thru XP, & limited support for Mac OS & Linux.
- Researched errors & defects to resolve customer technical issues.
- Initiated fraud investigations for client accounts upon discovery of questionable activities of retail store employees, call center or other employees, or the clients themselves.
- Developed & share innovative problem-solving techniques.
- Accepted customer service overflow from other tiers as needed during peak periods.
- Transferred to Store #899 due to position being outsourced to India.

BEST BUY CORPORATION - Lansing, Illinois & Orland Park, Illinois (8/01 to 11/02)

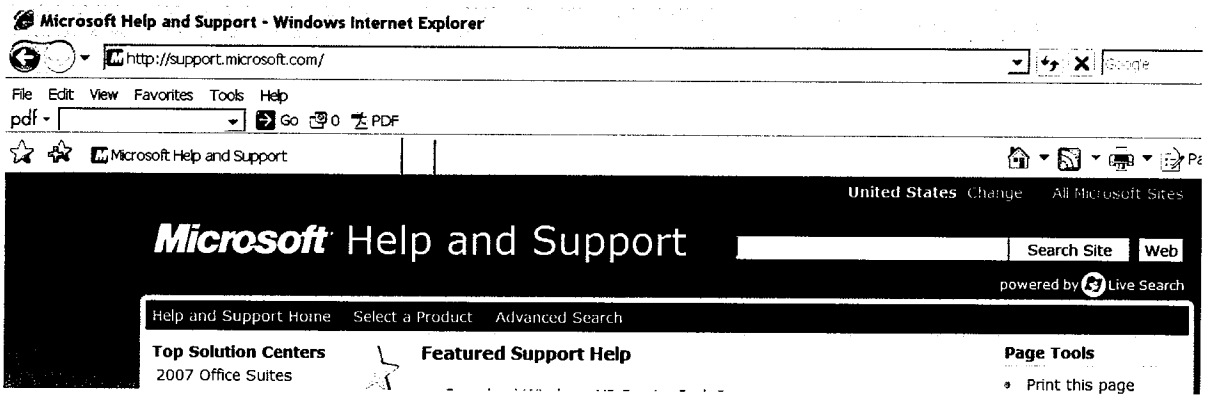
Senior Computer Repair Technician

- Repaired & maintained customer PCs running various Windows OS platforms.
- Installed peripherals such as disk drives, video cards, sound cards, hard-drives, network cards, & other devices in client computers.
- Provided in-store technical support for over 30 IBM NT4.0 workstations used for Point-Of-Sale & internal reporting as well as thermal printers and HP laser printers within store.
- Trained part-time technicians in new technologies & procedures for computer repair, software troubleshooting, & overall standard operating platform for the tech bench.
- Named "Tech Bench MVP" in November 2001 for customer service & technical leadership.
- Promoted to Senior Computer Repair Technician at Lansing location in July 2002.

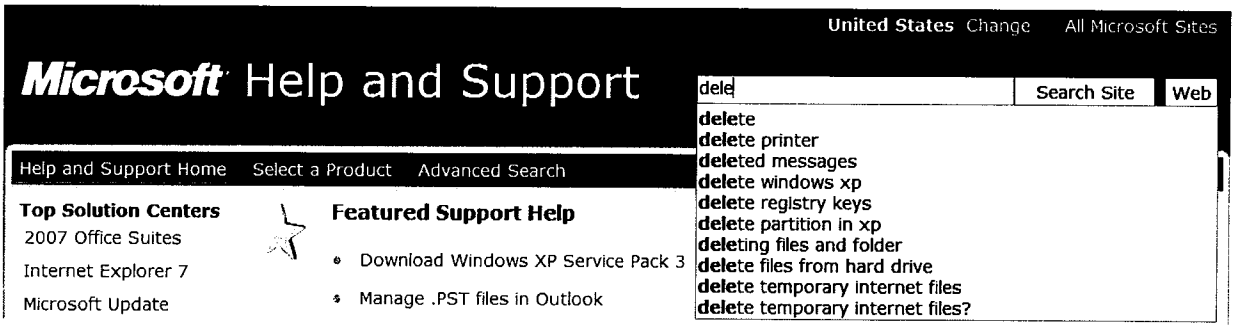
EXHIBIT B

Jones Affidavit – EXHIBIT B - Civil Action No. 08-cv-3939

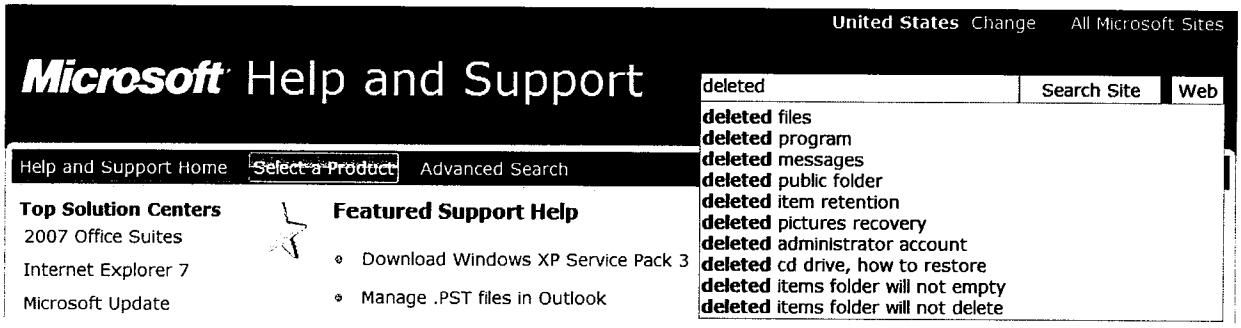
Website: http://support.microsoft.com



ID 2293 query = dele



ID 2291 query = deleted



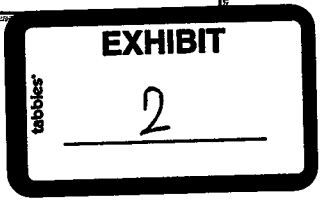
Jones Affidavit – EXHIBIT B - Civil Action No. 08-cv-3939

IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MINTEL INTERNATIONAL GROUP, LTD., a United Kingdom corporation,	)	
Plaintiff,	)	
-vs -	)	No. 08 CV 3939
MEESHAM NEERGHEEN, an individual	)	
Defendant.	)	

The videotaped deposition of MEESHAM NEERGHEEN, called for examination pursuant to notice and the Rules of Civil Procedure for the United States District Courts pertaining to the taking of depositions, taken before Allison D. Weber, CSR, a notary public within and for the County of Cook and State of Illinois, at 33 West Monroe Street, Suite 2700, Chicago, Illinois, on the 13th day of August, 2008, at the hour of 9:44 o'clock a.m.

Reported by: Allison D. Weber, CSR
License No.: 084-002238



Page 46

returned home?
A. I did.
Q. You're being represented by counsel here today; is that right?
A. Yes.
Q. And when did you -- when were you first represented by counsel in this matter?
A. I can't recall the date.
Q. Would it have been on that Monday, the 14th?
A. I don't know. I was told to go home and we'll get back in touch with you as to when you can come back into the office.
Q. When did you first hear from any of the lawyers at Bell, Boyd and Lloyd?
A. I believe -- oh, that's a very good question. I can't remember. I guess it probably was the Tuesday. It might have been the Wednesday.
Q. You know that there was a court hearing on the 16th, which was the Wednesday; is that right?
A. Yes.
Q. And I assume you spoke to your lawyers

Page 47

before that?
A. Okay. So it would have been either Monday afternoon or maybe Tuesday.
Q. Aside from -- and I'll caution you, I don't want to know the content of any conversations that you had with counsel or when counsel was present.
Besides your conversation with Mr. Howard, did you have any conversations with anyone else at Datamonitor regarding this lawsuit on the 14th or 15th?
A. No.
Q. Any conversations with anyone at Datamonitor prior to the court hearing on the 16th?
A. No.
Q. So it was just the one conversation with Mr. Howard on the 14th; is that right?
A. Yes, the Monday -- oh, I first spoke with him on the Saturday and then...
Q. Understood.
Did you do anything with your laptop computer upon receiving a copy of the summons and complaint?

Page 48

A. Did I do anything?
Q. Did you stop using it?
A. My laptop?
Q. Yes.
A. I think I may have printed out the documents just so that I could have a copy, because when I brought the copy that was delivered by messenger into the office, I left it with Richard Watkins.
Q. Did you keep using your computer?
A. No. No.
Q. You stopped using it entirely after --
A. Well, I was checking e-mails, yes, but -- I was using the internet to check e-mails because we -- I was liaisoning with -- I was liaisoning with my attorneys.
Q. Did you delete any documents from your computer from the time you received the complaint until the time you turned it over to counsel?
A. No.
Q. Aside from accessing the internet -- using the internet to access your e-mail, did you do anything else with the computer, run any other

Page 49

programs, anything like that?
A. No.
Q. I assume that Datamonitor -- someone at Datamonitor is the one that put you in touch with Bell, Boyd and Lloyd; is that right?
A. Yes.
Q. And who is paying Bell, Boyd and Lloyd's fees for this litigation?
MR. ROACHE: Objection, relevance.
You can answer.
THE WITNESS: I guess Datamonitor.
BY MR. PIOLI:
Q. Do you have an agreement with Datamonitor that they're going to pay the fees in this case?
A. No. No, I -- I don't recall signing anything that says that they're going to pay the fees.
Q. But that's your understanding?
A. That's -- I have been told that it's going to be handled, so...
Q. Who told you that?
A. My attorneys.
Q. So you're not worried at all that you're

Page 142

A. Can you define conversation?
Q. Sure. Let's start, have you had any oral communications with Mr. Cooper?
A. Yes, we have spoken, yes.
Q. Since you started at Datamonitor?
A. We have spoken, yes.
Q. What -- I'm sorry.
A. On a social basis, hi, hello, how are you.
Q. Did you have any discussions about Mintel with Mr. Cooper since you started at Datamonitor?
A. No.
Q. You previously testified that you did not know how to partition a hard drive; is that correct?
A. That's true.
Q. Do you know how big the hard drive is on your Sony computer?
A. I don't know.
Q. Does 30 gigabytes sound about right?
A. I don't know.
Q. Do you have any explanation as to why the hard drive on your computer is partitioned so

Page 143

that only 10.3 gigabytes is being used?
A. I don't know.
Q. Do you have any explanation as to why there's so many hard drives partitioned so that 17 gigabytes of unused space was deleted?
A. I don't know.
Q. You previously testified that only you and your attorneys had access to your computer since the time that this lawsuit was filed; is that correct?
MR. ROACHE: Objection, mischaracterizes his testimony.
He can answer.
THE WITNESS: Yes.
BY MR. PIOLI:
Q. Is that true, only you and your attorneys have access to your computer since this lawsuit was filed?
A. Yes.
Q. You previously testified that you only -- since the time the lawsuit was filed you only used the computer to access e-mail via the internet; is that right?
A. Yes.

Page 144

Q. Do you know what a defrag program is?
A. No.
Q. Are you aware that a defrag program was run on your computer on July 14th?
A. I don't know.
Q. Do you have any explanation as to why it would have been run on your computer on July 14th?
A. I don't know.
Q. Would it surprise you if a defrag program had been run on your computer on July 14th?
A. I don't know what a defrag program is.
Q. You're aware that an antivirus program ran on your computer on July 17th?
A. I don't know.
Q. You're aware that that would write over files?
A. I don't know.
Q. Are you aware of your duty to preserve evidence in this case?
A. I'm sorry?
Q. Are you aware of your duty to preserve

Page 145

evidence in this case?
A. Can you explain that?
Q. You're aware that once you had notice of this lawsuit you weren't supposed to be using your computer?
MR. ROACHE: Object to the form.
THE WITNESS: Um, I don't know.
BY MR. PIOLI:
Q. Nobody ever informed you about a duty to preserve evidence in this case?
A. I don't know.
Q. Isn't it true, sir, that on July 17th you accessed the Microsoft help and support website and entered queries about how to delete data from your computer?
A. Oh, I know exactly. Yes.
Q. Why did you --
A. It wasn't how to delete. I was trying to look for the files that I had sent over to my -- from my Mintel account, and I was trying to find out how to retrieve files from my Hotmail that had been deleted.
Q. What searches did you enter?
A. I can't remember.

Page 94

today?
A. My attorneys.
Q. Anyone besides your attorneys?
A. No.
Q. With regard to the -- we talked about the Dell computer that you had purchased from Mintel. Do you recall that?
A. Yes.
Q. When you sent it to your relative in Mauritius, did you receive any compensation for that?
A. No.
Q. Is it possible that that computer had Mintel information on it when you sent it to Mauritius?
MR. ROACHE: Objection, calls for speculation.
You can answer.
THE WITNESS: No.
BY MR. PIOLI:
Q. Why do you say it's not possible?
A. It was a home -- I wasn't using it. It was handed over as a gift.
Q. Am I right, I thought you previously

Page 95

testified that you had used it for some time.
A. Yes, for some time, but strictly just, you know, looking for my e-mails and just for general use, basically.
Q. You never did any work on that computer?
A. No.
Q. Never brought documents home to work on?
A. On that computer, no.
Q. Never accessed e-mail containing Mintel documents using that computer?
A. No.
Q. You're certain of that as you sit here today?
A. I'm certain. If ever I was doing any work, I take a loaner laptop from Mintel and I would work using the loaner Mintel laptop.
Q. And I apologize for being repetitive, but other than the Dell computer and the Sony laptop and the desktop computer you used at Mintel, did you use any other computers during your employment at Mintel?
A. No.

Page 96

Q. Do you know what a thumb drive is?
A. No. Thumb drive?
Q. Are you familiar with memory devices that you can connect through a USB port?
A. Yes.
Q. Okay. You're not aware that they're commonly called thumb drives?
A. No.
Q. What do you call them?
A. A flash drive.
Q. That's probably the better moniker for it.
During the time that you worked for Mintel, did you use flash drives to transport data between your work computer and your laptop?
A. Between my work computer and my laptop I don't know.
Q. It's possible that you did?
A. I once -- I guess I would -- I guess if the file was large enough, then, yes, I would transfer it to the flash drive.
Q. How many flash drives do you currently own?
A. Two.

Page 97

Q. Did you previously own more?
A. No.
Q. So is it your testimony that from the time you began work at Mintel's Chicago office until today you have only used two flash drives?
MR. ROACHE: Objection, mischaracterizes his testimony.
You can answer.
THE WITNESS: Yes.
BY MR. PIOLI:
Q. Did you ever use any CDs to transport documents from your work computer at Mintel to your laptop?
A. Yes. There was -- there were times when I would have presentations loaded up on to CDs as a backup, yes.
Q. Do you currently possess any CDs with Mintel's files or information on them?
A. No.
Q. Did you turn those in when you ceased your employment with Mintel?
A. They were left at work, so...
Q. You didn't have any at home?
A. No.

Page 90

Q. When did you receive your first paycheck from Datamonitor?
A. I don't -- sometime in June, I believe.
Q. What did you do between April 30th and May 27th?
MR. ROACHE: Object to the form.
You can answer.
THE WITNESS: I was enjoying the summer.
BY MR. PIOLI:
Q. Did you do any work on behalf of Datamonitor between April 30th, 2008 and May 27th, 2008?
A. No.
Q. Did you work daily for Datamonitor between May 27th, 2008 and July 14th, 2008 when Mr. Howard instructed you to go home?
A. Did I work daily?
Q. Yes.
A. Yes.
Q. After you went home on July 14th, 2008, did you do any work on behalf of Datamonitor?
A. No.
Q. Have you resumed your work for Datamonitor?

Page 91

A. Yes.
Q. When did you resume working for Datamonitor?
A. I can't remember. Towards the end of -- I really can't remember.
Q. Was it during the month of July?
A. Yes.
Q. Was it more than a week that you were out of work?
A. Yes.
Q. Was it more than two weeks?
A. No.
Q. Who fulfilled your job responsibilities while you were out of work?
A. I don't know.
Q. When did your work visa with Mintel expire?
A. I think it's still valid, so it was still valid when I was still at Mintel.
Q. Was it your understanding that your Mintel work visa was transferable?
MR. ROACHE: Objection to the extent it calls for a legal conclusion.
THE WITNESS: I don't know.

Page 92

BY MR. PIOLI:
Q. You previously testified that you had turned over your Sony -- Mintel Sony laptop computer to counsel; is that correct?
A. Yes.
Q. When did you do that?
A. I'm not sure of the exact date.
Q. Was it prior to the TRO hearing on July 16th?
A. I can't remember.
Q. Was it more than a week after you were served with a summons and complaint in the case?
MR. ROACHE: Objection, asked and answered.
You can answer.
THE WITNESS: I don't know. I don't know the exact date.
BY MR. PIOLI:
Q. Was it a matter of days or weeks that you turned it over to counsel?
A. I don't know.
Q. Was it a month before you turned it over to counsel?

Page 93

A. No, it was most definitely less than a month.
Q. Was it more than three weeks?
A. No.
Q. Was it more than two weeks?
A. I don't think so.
Q. Was it less than a week?
A. It could have been a week. It could have been less than a week. I know for sure it was not two, three or four weeks after.
Q. From the time that you were served with the lawsuit on July 11th until today, has anyone had possession and control over your computer other than either yourself or counsel?
A. No.
Q. And when you log on to your computer, you have a user name; is that right?
A. Yes.
Q. And you have to type in a password as well?
A. Yes.
Q. And did anyone have access to your user name and password from the time you were served with a copy of the summons and complaint until

today?
A. My attorneys.
Q. Anyone besides your attorneys?
A. No.
Q. With regard to the -- we talked about the Dell computer that you had purchased from Mintel. Do you recall that?
A. Yes.
Q. When you sent it to your relative in Mauritius, did you receive any compensation for that?
A. No.
Q. Is it possible that that computer had Mintel information on it when you sent it to Mauritius?
MR. ROACHE: Objection, calls for speculation.
You can answer.
THE WITNESS: No.
BY MR. PIOLI:
Q. Why do you say it's not possible?
A. It was a home -- I wasn't using it. It was handed over as a gift.
Q. Am I right, I thought you previously

testified that you had used it for some time.
A. Yes, for some time, but strictly just, you know, looking for my e-mails and just for general use, basically.
Q. You never did any work on that computer?
A. No.
Q. Never brought documents home to work on?
A. On that computer, no.
Q. Never accessed e-mail containing Mintel documents using that computer?
A. No.
Q. You're certain of that as you sit here today?
A. I'm certain. If ever I was doing any work, I take a loaner laptop from Mintel and I would work using the loaner Mintel laptop.
Q. And I apologize for being repetitive, but other than the Dell computer and the Sony laptop and the desktop computer you used at Mintel, did you use any other computers during your employment at Mintel?
A. No.

Q. Do you know what a thumb drive is?
A. No. Thumb drive?
Q. Are you familiar with memory devices that you can connect through a USB port?
A. Yes.
Q. Okay. You're not aware that they're commonly called thumb drives?
A. No.
Q. What do you call them?
A. A flash drive.
Q. That's probably the better moniker for it.
During the time that you worked for Mintel, did you use flash drives to transport data between your work computer and your laptop?
A. Between my work computer and my laptop I don't know.
Q. It's possible that you did?
A. I once -- I guess I would -- I guess if the file was large enough, then, yes, I would transfer it to the flash drive.
Q. How many flash drives do you currently own?
A. Two.

Q. Did you previously own more?
A. No.
Q. So is it your testimony that from the time you began work at Mintel's Chicago office until today you have only used two flash drives?
MR. ROACHE: Objection, mischaracterizes his testimony.
You can answer.
THE WITNESS: Yes.
BY MR. PIOLI:
Q. Did you ever use any CDs to transport documents from your work computer at Mintel to your laptop?
A. Yes. There was -- there were times when I would have presentations loaded up on to CDs as a backup, yes.
Q. Do you currently possess any CDs with Mintel's files or information on them?
A. No.
Q. Did you turn those in when you ceased your employment with Mintel?
A. They were left at work, so...
Q. You didn't have any at home?
A. No.

AO88 (Rev. 12/06) Subpoena in a Civil Case

Issued by the

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS

MINTEL INTERNATIONAL GROUP, LTD.

V.

MEESHAM NEERGHEEN

SUBPOENA IN A CIVIL CASE

Case Number:[1] 08 CV 3939

TO: Richard Watkins
Datamonitor
200 West Monroe Street
Chicago, IL 60606

☐ YOU ARE COMMANDED to appear in the United States District court at the place, date, and time specified below to testify in the above case.

PLACE OF TESTIMONY	COURTROOM
	DATE AND TIME

☐ YOU ARE COMMANDED to appear at the place, date, and time specified below to testify at the taking of a deposition in the above case.

PLACE OF DEPOSITION	DATE AND TIME

☑ YOU ARE COMMANDED to produce and permit inspection and copying of the following documents or objects at the place, date, and time specified below (list documents or objects):
SEE ATTACHED RIDER

PLACE	DATE AND TIME
Katherine J.Pronk, JOHNSON & BELL, LTD. 33 W. Monroe St., Suite 2700, Chicago, IL 60603	7/23/2008 5:00 pm

☐ YOU ARE COMMANDED to permit inspection of the following premises at the date and time specified below.

PREMISES	DATE AND TIME

Any organization not a party to this suit that is subpoenaed for the taking of a deposition shall designate one or more officers, directors, or managing agents, or other persons who consent to testify on its behalf, and may set forth, for each person designated, the matters on which the person will testify. Federal Rules of Civil Procedure, 30(b)(6).

ISSUING OFFICER'S SIGNATURE AND TITLE (INDICATE IF ATTORNEY FOR PLAINTIFF OR DEFENDANT)	DATE
Joseph R. Marconi (by: KJP)	7/21/08

ISSUING OFFICER'S NAME, ADDRESS AND PHONE NUMBER
Joseph R. Marconi, JOHNSON & BELL, LTD.
33 W. Monroe St., Suite 2700, Chicago, IL 60603 312/984-0211

(See Rule 45, Federal Rules of Civil Procedure, Subdivisions (c), (d), and (e), on next page)

[1] If action is pending in district other than district of issuance, state district under case number.

EXHIBIT 3 tabbies

AO88 (Rev. 12/06) Subpoena in a Civil Case

PROOF OF SERVICE

DATE	PLACE
SERVED 7/21/2008	Datamonitor 200 West Monroe Street, Chicago, Illinois 60606
SERVED ON (PRINT NAME) Richard Watkins	MANNER OF SERVICE Messenger Delivery
SERVED BY (PRINT NAME)	TITLE Messenger

Demetrius Witt

DECLARATION OF SERVER

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Proof of Service is true and correct.

Executed on 7/21/2008
DATE

Demetrius Witt
SIGNATURE OF SERVER

Johnson & Bell, Ltd.
ADDRESS OF SERVER

33 W. Monroe St., Suite 2700, Chicago, IL 60603

Rule 45, Federal Rules of Civil Procedure, Subdivisions (c), (d), and (e), as amended on December 1, 2006:

(c) PROTECTION OF PERSONS SUBJECT TO SUBPOENAS.

(1) A party or an attorney responsible for the issuance and service of a subpoena shall take reasonable steps to avoid imposing undue burden or expense on a person subject to that subpoena. The court on behalf of which the subpoena was issued shall enforce this duty and impose upon the party or attorney in breach of this duty an appropriate sanction, which may include, but is not limited to, lost earnings and a reasonable attorney's fee.

(2) (A) A person commanded to produce and permit inspection, copying, testing, or sampling of designated electronically stored information, books, papers, documents or tangible things, or inspection of premises need not appear in person at the place of production or inspection unless commanded to appear for deposition, hearing or trial.

(B) Subject to paragraph (d)(2) of this rule, a person commanded to produce and permit inspection, copying, testing, or sampling may, within 14 days after service of the subpoena or before the time specified for compliance if such time is less than 14 days after service, serve upon the party or attorney designated in the subpoena written objection to producing any or all of the designated materials or inspection of the premises — or to producing electronically stored information in the form or forms requested. If objection is made, the party serving the subpoena shall not be entitled to inspect, copy, test, or sample the materials or inspect the premises except pursuant to an order of the court by which the subpoena was issued. If objection has been made, the party serving the subpoena may, upon notice to the person commanded to produce, move at any time for an order to compel the production, inspection, copying, testing, or sampling. Such an order to compel shall protect any person who is not a party or an officer of a party from significant expense resulting from the inspection, copying, testing, or sampling commanded.

(3) (A) On timely motion, the court by which a subpoena was issued shall quash or modify the subpoena if it

(i) fails to allow reasonable time for compliance;

(ii) requires a person who is not a party or an officer of a party to travel to a place more than 100 miles from the place where that person resides, is employed or regularly transacts business in person, except that, subject to the provisions of clause (c)(3)(B)(iii) of this rule, such a person may in order to attend trial be commanded to travel from any such place within the state in which the trial is held;

(iii) requires disclosure of privileged or other protected matter and no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) If a subpoena

(i) requires disclosure of a trade secret or other confidential research, development, or commercial information, or

(ii) requires disclosure of an unretained expert's opinion or information not describing specific events or occurrences in dispute and resulting from the expert's study made not at the request of any party, or

(iii) requires a person who is not a party or an officer of a party to incur substantial expense to travel more than 100 miles to attend trial, the court may, to protect a person subject to or affected by the subpoena, quash or modify the subpoena or, if the party in whose behalf the subpoena is issued shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship and assures that the person to whom the subpoena is addressed will be reasonably compensated, the court may order appearance or production only upon specified conditions.

(d) DUTIES IN RESPONDING TO SUBPOENA.

(1) (A) A person responding to a subpoena to produce documents shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the demand.

(B) If a subpoena does not specify the form or forms for producing electronically stored information, a person responding to a subpoena must produce the information in a form or forms in which the person ordinarily maintains it or in a form or forms that are reasonably usable.

(C) A person responding to a subpoena need not produce the same electronically stored information in more than one form.

(D) A person responding to a subpoena need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or to quash, the person from whom discovery is sought must show that the information sought is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) (A) When information subject to a subpoena is withheld on a claim that it is privileged or subject to protection as trial-preparation materials, the claim shall be made expressly and shall be supported by a description of the nature of the documents, communications, or things not produced that is sufficient to enable the demanding party to contest the claim.

(B) If information is produced in response to a subpoena that is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The person who produced the information must preserve the information until the claim is resolved.

(e) CONTEMPT. Failure of any person without adequate excuse to obey a subpoena served upon that person may be deemed a contempt of the court from which the subpoena issued. An adequate cause for failure to obey exists when a subpoena purports to require a nonparty to attend or produce at a place not within the limits provided by clause (ii) of subparagraph (c)(3)(A).

RIDER

Plaintiff Mintel International Group, Ltd. ("Mintel"), pursuant to Federal Rule of Civil Procedure 45, hereby requests that Datamonitor produce the following documents in its possession, custody or control, in accordance with the terms of the attached subpoena.

Definitions and Instructions

1. As used herein, "document" means any writing, graphic matter or other tangible thing, whether printed, electronically stored, recorded, produced by any process, or written or produced by hand, including, but not limited to checks, drawings, invoices, letters, reports, other written communications, correspondence, e-mails, telegrams, internal and external memoranda, summaries, records or oral conversations, original or preliminary notes, diaries, calendars, analyses, projections, ledgers, work papers, photographs, tape recordings, video tapes, computer hard drivers or disks, statistical statements, logs, graphs, charts, schedules, notebooks, minutes or records of meetings, minutes or records of conferences, lists of persons attending meetings or conferences, reports and/or summaries of investigations, opinions or reports of investigators, accountants or consultants, studies, appraisals, evaluations, or copies of any of the foregoing if the copy is in any way different from the original now in your possession, custody or control, or the possession, custody or control of your counsel, evaluation consultants, agents, employees and/or persons acting on your behalf.

2. If information or a document is withheld for any reason, identify the information or document and the reason for withholding the responsive information or document as follows:

(a) The reason for withholding the document, including an explanation of any privilege which is claimed;

(b) The date(s) of the document(s);

(c) The name and address of the author(s) of the document(s);

(d) The name and address of each person to whom a copy of the document(s) was sent and each person known to have seen or participated in communication about the document(s);

(e) The title, nature and subject matter of the information or document(s);

(f) The name, address and job title of each person who has possession, custody or control of such information or document(s);

(g) The present or last known location and custodian of the document(s); and

(h) All other information necessary to assess a claim of privilege.

3. In construing these requests:

(a) The singular form of a word includes the plural form and vice versa; and

(b) "And" and "or" are to be construed either disjunctively or conjunctively as is necessary to bring within the scope of each request any matter, information or document that might otherwise be construed as outside its scope.

4. As used herein, "Datamonitor" shall include all employees, directors, officers, agents, and individuals subject to Datamonitor's direction and control. In addition, "Datamonitor" shall include all parents companies, affiliates and subsidiaries.

Documents and Objects

1. Produce all documents representing, containing, reflecting or referencing any oral or written communications and/or correspondence between Datamonitor and Meesham Neergheen.

2. Produce all documents representing, containing, reflecting or referencing Meesham Neergheen's interview(s) with Datamonitor prior to Datamonitor's offer of employment.

3. Produce Meesham Neergheen's entire personnel file.

4. Produce any and all documents within Datamonitor's possession pertaining or relating to or otherwise referencing in any manner Meesham Neergheen.

5. Produce all documents, including correspondence, that refer to, relate to or otherwise constitute Meesham Neergheen's authorization to work in the United States of America.

6. Produce all documents, including correspondence, that refer to Meesham Neergheen's status as an immigrant in the United State of America.

7. Produce all documents, including correspondence, that refer to, relate to or constitute the means of Meesham Neergheen's entry into the United States of America.

8. Permit the forensic imaging and/or copying of all of Datamonitor's desktop and/or laptop computers used at any time by Meesham Neergheen.

9. Permit the forensic imaging and/or copying of Meesham Neergheen's electronic mail account at Datamonitor.